USDA

United States Department of Agriculture

Office of the Chief Information Officer

1400 Independence Avenue SW

Washington, DC 20250

DEC 14 2007

TO: Agency Chief Information Officers

FROM: Charles R. Christopherson, Jr.
Chief Financial Officer
Chief Information Officer

SUBJECT: USDA Password Policy

This memorandum supersedes all previous password policy memorandums and ensures compliance with forthcoming Federal Desktop Core Configuration (FDCC) requirements. Agencies should begin to implement these requirements immediately and have until February 1, 2008 to achieve full compliance. Agencies should establish controls to enforce the following password settings for all user accounts:

- Sixty days maximum age limit;
- One day minimum age limit;
- Twelve or more characters in length;
- Alpha, numeric, and special character combination (Complexity turned on);
- No dictionary words;
- Five failed login attempts; and
- A history of 24 previously used passwords.

System administrators should have at least two accounts, one account for system administration access and one for common network access such as e-mail and Internet access. Accounts used for system administration tasks should not be mail or Internet enabled.

Those systems that cannot meet these password requirements are required to use the maximum password requirements the systems will allow. Agencies are required to ensure that the password limitations are fully documented in their certification and accreditation documents.

Blackberry devices are required to lock after 30 minutes and require a password to be unlocked. The password must meet the following guidelines.

- A minimum of five characters must be used, at least one letter (lower or upper case) and one number must be used (the Blackberry Enterprise Server (BES) must be configured to enforce this policy);
- If six or more characters are used, the password may contain only numbers;
- A maximum of ten failed password attempts before the device is wiped (the BES must be configured to enforce this policy); and
- Passwords must be changed every 90 days.

Establish procedures to remotely wipe all lost or stolen Blackberry devices upon notification.

For Personal Data Assistants that employ Palm OS Version 5 Garnet and Version 6 Cobalt, the device password protection should be set to automatically lock the device on power off and after 15 minutes of inactivity.

Windows Mobile devices including Pocket PCs are required to have a password policy that meets the following requirements:

- Eight or more characters;
- Combination of letters and numbers;
- Number of incorrect password attempts set to three before the device is wiped; and
- Lock the device after 15 minutes of inactivity.

Please contact the Security Compliance Division at 816-823-2377 or cyber.communcation@usda.gov for questions or comments regarding this memorandum.